MCF

Michael C. Farkas, Esq., PLLC

381 Park Avenue South • 16th Floor • New York, New York 10016
Dir: 212.760.8400 • Gen: 212.779.8600 • Fax: 212.760.8403 • mfarkas@farkaslawfirm.com

June 1, 2009

Via Electronic Filing

Hon. Nancy Gertner
United States District Judge
District of Massachusetts
One Courthouse Way
Boston, MA 02210

Re: United States v. Stephen Watt
08-CR-10318-NG

Dear Judge Gertner:

I represent Stephen Watt ("Watt"), the defendant in the above-referenced indictment. Please accept this letter as Watt's sentencing memorandum. Watt is scheduled to appear before Your Honor to be sentenced on June 8, 2009, pursuant to his conviction upon a plea of guilty to Conspiracy, in violation of 18 U.S.C. §371. When he appears before Your Honor on that date, Watt will be the first, and least culpable, member of the conspiracy at issue to be sentenced in this District.

Watt seeks a probationary sentence or, in the alternative, a minimal sentence of incarceration, based upon the factors to be considered in imposing a sentence pursuant to 18 U.S.C. §3553(a) and Watt's objections to the government's and U.S. Probation Office's offense level calculations. Watt's requests for consideration and, if applicable, departures from the U.S. Sentencing Guidelines ("Guidelines") are supported among other things by the fact that the recommended offense level, particularly with regard to loss calculation under U.S.S.G. §2B1.1(b)(1), severely overstates his culpability in this matter as well as the likelihood that he will commit future crimes.

Watt is a unique participant in this enterprise in that he is the only conspirator not alleged to have committed a computer intrusion of any kind, trafficked in any unauthorized access device, or "moved" or collected a percentage of the proceeds gleaned from this conspiracy. Moreover, before federal agents executed search warrants at his office and home (resulting in his termination from his job), Watt was the only

gainfully employed member of the conspiracy, with a bright future and a promising career ahead of him in a computer-related field within the securities and financial services industries.[1] In his early 20's during the period relevant to the instant allegations, Watt was (and remains) an intellectually gifted young man whose academic fascination with computer network intrusions (i.e. "hacking") became his undoing. His immature and ill-advised discourse with his close friend, Albert Gonzalez, has now, at the least, severely damaged the future that he had so carefully built over his years of schooling and work. While the support Watt provided to Gonzalez in this case was of an elementary nature, without the benefit of knowing the true extent of what Gonzalez was doing, it was still sufficient to render Watt criminally responsible to some degree in this matter and detrimentally affect him for the rest of his life. It should not, however, result in even more devastating consequences in the form of substantial incarceration.

I. Defendant's Background History and Characteristics

The Pre-Sentence Investigation Report ("PSR") prepared by the U.S. Probation Office accurately recites some of Watt's background. He was born on July 1, 1983 and raised in Florida by his parents, who grew up outside of the United States (Watt's father was raised in Canada, while his mother was raised in the former Yugoslavia). As a result, Watt is fluent in Serbo-Croatian. He also taught himself to be somewhat conversant in Italian.

Watt was, and, to a great extent still is, an introvert. He had few friends while growing up and quietly chose instead to concentrate on academics, primarily though reading books and using/learning computers, and playing sports. His preferred social isolation is probably due as much to his advanced intellect as his striking physical features: Watt stands seven feet tall and has always been an imposing figure, even in childhood. He grew very quickly and was always awkward, especially for someone who graduated high school at the age of 16 and college at the age of 19. Although it may come as a surprise to many who see him today, Watt's voracious appetite for reading and learning led him to amass an extraordinary foundation of knowledge at a young age.

Watt graduated high school in 2000 with a 4.37 grade point average (he surpassed the traditional 4.0 limit through honors and advanced placement classes, the latter of which earned him substantial college credits). He received a full National Merit scholarship and attended college in Florida, where his overall GPA was between 3.5 and 4.0. He majored in liberal studies and minored in computer information technology. Prior to college, Watt's computer skills were entirely self-taught. He received his bachelor's degree in 3 years.

Before college, Watt spent his last two high school summers working for a computer software company in Florida (Identitech). During the summers of 2001 and 2002, Watt worked for another software company (Qualys) as a software developer and

[1] Recently, however, two individuals with legitimate jobs have been charged in this matter: Jeremy Jethro and Humza Zaman. Their roles in this conspiracy, although more limited that the main actors, are still greater than Watt's.

engineer, in that company's California and Paris offices. In addition to France, Watt has traveled extensively throughout Western Europe and North America.

After graduating from college Watt moved to New York in late 2003. While looking for his first full-time job as a new college graduate, Watt did what he could to earn income. He was employed full-time for several months with a contractor, doing demolition work on commercial construction sites and earning $9 an hour. He also did a couple of contract computer jobs (one performing network administration, the other doing computer forensics investigations). All the while, Watt was interviewing with prospective employers. He was finally hired by Morgan Stanley in or about May of 2004 as a software engineer. Watt earned total compensation of about $99,000 per annum in that position. These details are important not only to illustrate his diligent work ethic, but also to provide context for the acts he committed in this case: during the time that he was finishing college, then "breaking rocks" to stay employed, and finally securing his first job in his chosen field, Albert Gonzalez was committing significant computer-related crimes. Watt's priorities were obviously elsewhere.

Watt's computer work within the securities industry led to a nascent career within a specialized niche field. He left Morgan Stanley in early 2007 to take a higher-paying position with a private company, Imagine Software, where Watt began developing software such as real-time computer trading programs for financial firms. Watt now earned about $130,000 in total annual compensation and was well on his way to a long-term future developing complex software systems for the financial services industry.

On August 13, 2009 that future ended with the execution of a federal search warrant at Watt's place of business. He was fired by Imagine Software and effectively banned from working within the securities industry (a literal ban has now resulted from his felony plea, as he cannot obtain employment as a convicted felon with any company doing business within that highly regulated industry). The dire impact upon Watt's professional and personal life cannot be overstated: whenever he is permitted to use a computer again, he will have to start over in a new area within the software engineering field, hoping that his felony conviction will not permanently prevent him from securing a position with a future as promising as the arena he forfeited. Until he can use a computer, he has no hope of finding any substantive work at all. Watt has collected unemployment payments since he lost his job, together with some financial assistance from his mother.

Watt met Albert Gonzalez online while Watt was in high school. Gonzalez is three years older than Watt. The two shared a keen interest in computers, particularly network security and vulnerabilities within such systems, which is a highly technical and challenging genre that intrigued Watt from a young age. Gonzalez became Watt's close friend, one of the very few that Watt had. As will be detailed later, Watt's fascination with this area was best described as being on a mischievous and intellectual level. Gonzalez, on the other hand, proved to be more interested in harmful and profitable criminal behavior than in casual "hacking."

In or about late 2004, after he had moved to New York City and after he broke up with his girlfriend of approximately 3 years, Watt began experimenting with recreational drugs. He initially began using them in social settings, such as nightclubs. As he had done with his other "interests" earlier in life, Watt approached this experimentation with an intellectual curiosity and discipline that would seem surprising to most objective observers. While not "addicted," Watt nevertheless acknowledges that his drug use started to become problematic as his father was dying of cancer and before he began another relationship with a girlfriend in mid-2006 to early 2007. Since then, and especially since meeting his wife in late 2007, Watt's use became more limited. Watt has completely refrained from any drug use of any sort since he submitted to pre-trial supervision in December of 2008, without the benefit of any counseling. Clearly, he was well on his way to "growing out of it" and now has no difficulty abstaining completely.

Watt's substantial experimentation with uncommon, hallucinogenic substances is perhaps analogous to his intellectual curiosity with, and the stimulation gained from, the excitement surrounding exploitation of computer network vulnerabilities. Both are indicative of an immature fascination with, for lack of a better phrase, "forbidden fruit." Again, unlike in the case of Gonzalez, this mischievous fascination seems to have perpetuated alongside a failure to appreciate the consequences of such actions.

I urge your honor to read the attached letters from Watt's family and friends (annexed hereto as **Exhibit A**). They provide a rich description of my client, one that portrays a warm, selfless, and extraordinary individual who had much to offer society, but who has now become depressed and downtrodden about his future prospects. While it is no stretch for many criminal defendants to provide character references, a reading of the attached letters conveys a compelling portrait about Watt that I believe is critically relevant to your determination in this matter.

II. Defendant's minimal involvement in this conspiracy

In pleading guilty herein, Watt has admitted to editing and providing Gonzalez with a "sniffer" program that Gonzalez and his co-conspirators then used to capture data from the networks that they intruded upon. Watt is not alleged to have committed, nor did he ever commit, any network intrusions in furtherance of this conspiracy. He is similarly not alleged to have supported the conspiracy in any other way (e.g. by providing other technical assistance, by trafficking stolen debit or credit card data or identity information, by physically helping to launder money, etc.) nor is he alleged to have profited financially from this conspiracy. A question for Your Honor's determination in this sentencing matter, therefore, is to what extent (if any) has the government demonstrated that Watt knew of Gonzalez's designs with regard to that "sniffer" program.

The answer to that question, however, stands firmly apart from the elementary and extremely limited nature of the assistance that Watt provided to him. Watt submits that no matter what Your Honor's ultimate determination may be with regard to Watt's knowledge (which, as detailed below, he avers to have been minor), the nature of the

work performed by Watt on the "sniffer" program is of such a relatively inconsequential nature as to render Watt's overall culpability in this matter to be minimal. In short, at the end of the day, Watt provided a simple and readily available piece of software to Gonzalez and nothing more. Even the government's statement of offense conduct illustrates this point, as it devotes substantial attention to the other members of the conspiracy and relatively little time on Watt's limited actions.

The foregoing forms the basis for Watt's legal challenges to the Guidelines calculations in this matter, as well as his prayer for consideration under 18 U.S.C. §3553(a). This memorandum first address the former, beginning with an explanation of "sniffer" programs in general and the program specifically involved in this case. A review of Watt's knowledge relating to Gonzalez and his scheme follows, analyzing the question of what was "reasonably foreseeable" to Watt. The totality of the government's circumstantial evidence relating to Watt's knowledge (or lack thereof) is also examined. A review is then conducted of the other defendants involved herein and their infinitely more substantial acts committed in furtherance of this conspiracy as compared to Watt. This memorandum then details Watt's plea in Section III, the PSR and Watt's objections thereto in Section IV, and then Watt's analysis of the 18 U.S.C. §3553(a) factors in Section V.

1. The "sniffer" program and its limited significance in this case

A program known as a "sniffer" refers to a class of application that captures any type of data that travels across a communications network. "Packet sniffers" are the most commonly referenced, which are used to capture and often store data that travel across a local network or the Internet. Sniffers serve a wide variety of purposes and can be used in many sorts of legitimate research, diagnostics, and security-related scenarios, in addition to illegal data gathering.[2]

There are literally hundreds of different sniffers that are available on the Internet for download. Most of these are free, although some more sophisticated versions are resold commercially. Additionally, any number of tutorials on the construction of sniffers can be found in well-respected software development magazines, which are used to provide a practical example for the programmer interested in gaining a deeper knowledge of network programming fundamentals. Some easily obtainable sniffers target data

[2] For example, programmers involved in the development of Internet-capable applications frequently use sniffers to monitor the output of these applications to verify that the content of the data actually being sent across an Internet connection matches the intended output of the code that they have written. Network administrators might also use sniffers to verify that the firewall rules they have devised to protect their networks, or the routing configurations they have established to facilitate the flow of Internet traffic, are indeed allowing and/or impeding the transmission of certain types of data across their network. Security administrators may use sniffers to check to see if their computer systems are using insecure unencrypted communications channels to transmit sensitive information across networks, which might be stolen by intruders. Finally, sniffers can also be appropriated for malicious activity, as they can also be used to capture information that travels across networks such as logins and passwords, transmitted files, and various forms of electronic conversations.

channels used by specific types of applications, such as web traffic, email, or instant messenger conversations. Other readily available sniffers operate in a much more general scope, and can be configured to blindly log virtually any type of data that falls within the parameters specified by the end-user of the sniffer.

The sniffer "blabla" involved in this case falls into this latter class of sniffers, which blindly logs any type of data. Specifically, it is known as a "raw TCP sniffer," which can be used to "sniff" incoming data to any sort of Internet server as it was not designed with the prescience of any target host computer or network. There are certainly other freely and legally available sniffer programs on the Internet which could have satisfied equally the same purpose of sniffing the credit card information in question, with minimal or no modification.

The complete knowledge necessary for the construction of a sniffer can be easily obtained through the research of various books on computer programming, operating system help manuals, or from the source code to any other freely available sniffer program, as the overwhelming majority of such programs are published with a policy of full disclosure that includes both source code and full documentation. To a security developer, the intrinsic code of the "blabla" sniffer would have been elementary and straightforward, and since the capabilities of the sniffer were so generic and flexible, it could have easily been tested on the same computer on which it was developed – that is to say it could have been written and fully tested on <u>any</u> computer, even one without any sort of network connection. The "blabla" sniffer probably does not constitute more than several hundred to less than a couple of thousand of lines of code. As a benchmark of how long this might take in full to develop, a competent programmer might average somewhere between 100-200 lines of code per hour. Consequently, a program such as "blabla" could be easily written from scratch in the span of a few hours to less than a full day. As most programmers recycle or copy applicable code from similar projects, resourceful code borrowing would likely reduce this conservative estimate significantly.

Accordingly, the sniffer involved in this matter is an elementary software tool that exists in substantially the same form in the public domain. Gonzalez asked Watt for a sniffer as a matter of convenience. Watt was his close friend, someone who would quickly and easily save Gonzalez the trouble of having to obtain a sniffer on his own or find someone else to do it for him. The technical assistance that Watt provided was not in itself indicative of some particularly grand scheme. The government argues that Watt's sniffer was "critical to the success of the massive identity theft which followed," and as such, was the instrumentality required by the conspirators to steal the massive amounts of data involved in this case. This argument is illusory, however, as Watt provided no particularly indispensible assistance that was critical to the conspiracy's success. An analogy that comes to mind is a plumber installing a drainpipe below a sink. To the plumber, that installation is elementary and could have been done by anyone having any experience with plumbing, or someone willing to learn; to the plumber's customer, the pipe is "critical to the success" of the water flowing out of the sink. Watt does not deny that he utilized a special skill in editing the sniffer for Gonzalez – he

simply challenges the purported indispensability of the sniffer, which certainly does not flow from such a skill in this instance.

Further demonstrating the elementary nature of Watt's assistance is the information gleaned from one of the government's cooperating witnesses, Damon Patrick Toey. Toey states that Gonzalez asked Watt to modify the sniffer during a party that they were attending in or about March of 2007. Watt, however, was under the influence of drugs at that party, and in his altered state he could not perceive the computer screen or keyboard well enough to make the necessary code changes. The modification requested by Gonzalez was so minor, and the sniffer program itself so simple, that Watt was nevertheless able to verbally instruct Toey (who is not an accomplished programmer) as to how to edit the limited lines of code needed to complete the modification. Watt is certainly not proud to admit to the Court that he was under the influence of drugs to this extent, however this example is illustrative of two key points: the sniffer's simple nature and composition, and the context in which Watt operated with regard to his "assistance" to Gonzalez. To Watt, this was borne out of immaturity and friendship, not a desire to steal.

For these reasons, it is improper to impute the full weight of responsibility for the conspirators' actions upon Watt in this matter, particularly with regard to the loss calculations proposed by the government under U.S.S.G. §2B1.1(b)(1). Doing so would also clearly overstate Watt's culpability herein.

2. Watt's lack of knowledge of Gonzalez's plans, and the Government's related evidence

Watt's limited knowledge of Gonzalez's plans further illustrates why the proposed Guidelines range cannot be applied in this matter, or how it would be unjust to do so. When Gonzalez requested that Watt provide and/or edit a sniffer program, Watt knew nothing about the intrusions committed in this case (e.g. TJX, Dave & Buster's, etc.). He did not profit from these intrusions, nor did he render any assistance relating to them beyond providing the sniffer. Watt certainly knew that Gonzalez was planning to use the sniffer in some sort of intrusion, and as the government has noted in its statement of offense conduct to the Probation Office, "chat logs" between Watt and Gonzalez from 2005 to April of 2006 indicate that Gonzalez had discussed intruding into large corporate networks for financial gain. Despite these facts, however, the government's evidence actually supports the fact that Watt knew nothing about the specific intrusions herein; that he did not access any information that would indicate otherwise; and that he had no specific information relating to the extent of Gonzalez's success.

Statements by the government's cooperating witness, Damon Patrick Toey, who the government has endorsed as credible, indicate that Watt "codes for Gonzalez more because they are friends" (as opposed to being "motivated by money"). Toey further stated that he did not believe Watt to be a major part of this conspiracy, other than coding sniffer programs. As stated above, Toey describes one incident at a party in or about March of 2007 where Gonzalez asked Watt to edit the sniffer. Toey does not provide any

indication that Watt knew why he was performing that task for Gonzalez, other than a general reference to the fact that they were "friends."

For what it is worth, Gonzalez also stated to the government that he did not tell Watt why he needed the sniffer program used in this case to facilitate the TJX data theft.

Turning to forensics, the government's evidence indicates that Watt frequently accessed a server in Latvia in late-2007 and January of 2008, and that on one occasion a newer version of the "blabla" sniffer was uploaded to a particular directory (called "Z") on that server less than one minute after Watt accessed said directory. This is the only forensic evidence in the government's possession implicating Watt. The government's forensics also indicate that an older version of the "blabla" sniffer was "compiled" on the Latvian server 45 minutes prior to a TJX intrusion on May 18, 2006, however no evidence (other than supposition) implicates defendant on such date. Further, the government's evidence conclusively establishes that the "Z" directory on the Latvian server was segregated from the other areas of that server, and that Watt did not have access to anything but the "Z" directory. In English, this means that Watt could not view or access anything on the Latvian server other than what was in the "Z" directory. As it happens, stolen credit and debit card and identity information was stored by the conspirators in those other areas of the Latvian server. Again, Watt had no ability to view or access those areas.

It must also be noted that the "chat logs" referenced by the government between Watt and Gonzalez date through April of 2006, one month before the TJX intrusion that uploaded the sniffer to its system, but also six months after Gonzalez and Scott had compromised TJX's system, stolen TJX data, and uploaded it to the California server. Despite the timing, nowhere in those logs is any mention made of TJX. A further discussion on the remainder of the "chat log" details appears later in this memorandum.

To summarize in the interim, the government's forensic evidence thus far suggests that Watt modified the "blabla" sniffer in late-2007 to early-2008 and uploaded it to the "Z" directory on the Latvian server, a suggestion that Watt does not dispute. It by no means, however, establishes that Watt knew that the sniffer was to be used to steal TJX data in 2006, or Dave & Buster's data in mid-2007 (in fact, Watt did not even have logon access to this server until late-2007). This is an impermissible leap that the government hopes the Court will make.

Additional forensic evidence indicates that Gonzalez utilized another server in California to store data stolen from TJX in September of 2005. The government appears to claim, circumstantially, that it has evidence that Watt had "access" to this server. This evidence consists of a piece of paper recovered by Federal agents in Watt's apartment in August of 2008. On this paper was printed an IP address that became the California server's IP address in December of 2005 (after the TJX data was uploaded), as well as a password corresponding to another server utilized by the "Shadow Crew" (which was a prior criminal enterprise operated by Gonzalez) and a file path leading to the file, "a.tar" (which the government cannot identify). From this document, the government concludes

in its statement of offense conduct, "at some point during the conspiracy, Gonzalez told Watt how to access the computer server to which Scott transferred large amounts of data from TJX in the fall of 2005." This is an erroneous conclusion. First and foremost, the government has *absolutely no evidence of Watt accessing the California server or the TJX data*, either in 2005 or at any time thereafter. Had Watt had such access, it would be proven forensically (as in the case of the Latvian server, mentioned above). Second, the document plainly indicates that Watt jotted down information on how to view a specific file, located on a particular server, at some point prior to August of 2008 (but, most likely, after March of 2007, when Watt moved in to that apartment). Because IP addresses change with such ease, and because the password on this document *did not correspond to the California server* as it was in 2005, there is no way to determine even circumstantially that Gonzalez gave Watt access information to the server where he was storing stolen TJX data back then. It seems obvious that Gonzalez told Watt how to access a file ("a.tar") on one of his servers, and nothing more. Such an act would be commonplace to Watt, who frequently accessed servers maintained by his friends to communicate securely and exchange files. Again, Gonzalez and Watt were close friends. "A.tar" could have been anything, and the government does not allege that it to be nefarious in any way. In sum, the government's "evidence" relating to this California server is a red herring.

It is also noteworthy that during the time that Gonzalez was operating the "Shadowcrew" enterprise in 2003, Watt was in college in Florida and then working demolition in New York to make ends meet. This is surely not the lifestyle of someone reaping huge financial rewards from online theft.

The government also has forensic evidence that Gonzalez and his accomplices utilized a server in Ukraine to store stolen data. For example, the PSR states at paragraph 45, "thus far, the Secret Service has recovered 27.5 million distinct credit card and debit card numbers from the server in Ukraine, and 16.3 million payment card numbers from the server in Latvia." As with the California server, however, and the areas of the Latvian server that contained the aforementioned data but were off-limits to Watt, the government has no evidence that Watt accessed or viewed any information on this Ukrainian server.

At this point it is clear that the government has no reliable forensic or testimonial evidence indicating that Watt had any specific knowledge of the objects of the Gonzalez conspiracy. What remains are the aforementioned "chat logs" between Watt and Gonzalez from February 2005 to April of 2006, and general references to other close contacts these friends maintained (by telephone, personal visits, and the extreme "partying" that they did together).

If Your Honor is inclined to read the nearly 300 pages of "chat" in this matter, you will note a distasteful, at times obscene, yet entirely juvenile discourse between two young men relating to topics ranging from music, to socializing in the "club" scene, to all manner of casual sexual exploits, to weightlifting, to computer "hacking." Watt does not deny that these were his interests at the time, especially earlier in his life (he was 21 to 22

years old during these chat sessions, living on his own in New York City). Watt also does not deny that Gonzalez spoke frequently of his more aggressive hacking activities, including his desire to gain access to and profit from large corporate networks such as bizrate.com, or that Watt participated in discussions with Gonzalez about how to gain such access. In nearly every instance, however, it is abundantly clear that Watt's focus during these discussions was on matters unrelated to the serious pursuit of such intrusions (e.g. music, weightlifting, sex, drugs, or any manner of other social topics). While Gonzalez often pushed Watt to assist him, Watt just as often changed the subject and discussed the aforementioned topics. This is not to say that Watt did not participate in these discussions or assist with solving "hacking" related problems – he did – but he did so from an intellectual and mischievous perspective of someone who was stimulated by the exercise. In fact, through Toey, the government has evidence that Gonzalez frequently complained that Watt was "*slow to make revisions to the sniffer when Gonzalez requested them.*" This theme continued throughout the chat logs, as Gonzalez continually chided Watt for blowing off Gonzalez's requests for assistance.

Watt's attitude towards these chats with his close friend is also consistent with someone who had other priorities in life, professionally as well as socially. In early 2005 when these chat sessions began, Watt had been working with Morgan Stanley for almost a year. Although the chat logs appear to be substantial, they represent fairly short daily periods of conversation, such as when Watt got up in the morning or returned from the gym (300 pages of chat over the course of more than one year is not voluminous). Watt was working full-time, weightlifting daily, and hosting multiple parties per week as a promoter. He did not have the time to devote to the kind of "hacking" that Gonzalez obviously was perpetrating. Indeed, the kind of illegal work that Gonzalez and his cohorts were doing require hours per day, for extremely long periods. Watt's interest in network intrusions remained, to be sure, but more as an intellectual stimulus. It is no coincidence that Watt was the only Gonzalez conspirator with a budding career and a bright future.

Watt's experimentation with recreational drugs also contributed to his close relationship with Gonzalez, who "partied" in much the same way and was generous with Watt when it came to hosting social events and using narcotics. The government will undoubtedly argue that the totality of these interactions, and the money that Gonzalez threw around for these parties, paint a clear picture of how Watt "knew" that Gonzalez was stealing tens or hundreds of millions of dollars from TJX and the other retailers involved in this matter.

This is another leap that cannot logically be made, however. At most, Watt knew or should have known that Gonzalez was seeking to "hack" into corporate networks in general, and that perhaps he had some success to an unknown extent. This type of supposition does not meet the government's burden to establish Watt's level of culpability, particularly with regard to the amount of loss that can be attributed to Watt under U.S.S.G. §2B1.1(b)(1). In any event, Watt knew that Gonzalez lived with his mother and had other sources of income. To conclude that Watt must have known that Gonzalez was stealing hundreds of thousands of dollars or more is simply illogical.

Most poignantly, however, is how neither the "chat logs" nor any other evidence indicates knowledge by Watt that TJX, Dave & Buster's, or any other retailer involved in this specific case was being victimized by Gonzalez, or to what extent. To the contrary, there is a distinct absence of such evidence, especially considering how Gonzalez had compromised TJX right in the middle of the period covered by the chat sessions. Accordingly, the level of culpability sought by the government cannot possibly be imputed to Watt based on speculation about what he might have "known."

3. The co-conspirators' obviously advanced roles as compared to Watt

As stated, Watt is by far the least culpable actor in this matter. More than that, he is the only defendant that did not take deliberate action to further either the logistical or pecuniary objects of this conspiracy. The limited references to Watt in the government's statement of offense conduct in the PSR amply illustrate these points.

Gonzalez's role has already been sufficiently discussed, both in the government's statement of offense conduct and within this memorandum. He is the "kingpin" in this case, responsible for the entirety of its repercussions both in this district and elsewhere. He is charged in this district in a 19-count indictment including Conspiracy and all underlying charges relating to it, and he faces a 27-count indictment in the Eastern District of New York for similar criminal conduct. Upon information and belief, well over $1 million has been recovered to date that can be attributed to Gonzalez's ill-gotten gains.

Christopher Scott pleaded guilty to a four-count Information charging Conspiracy and three underlying counts. Beyond the conduct described at length in the PSR, a review of his overt acts in furtherance of the conspiracy is informative. They include gaining unauthorized access to a BJ's Wholesale Club computer network with Gonzalez, and compromising track 2 data from that company; assisting Jonathan James with gaining unauthorized access to an OfficeMax network and downloading track 2 debit card data including encrypted PIN's, which they passed on to Gonzalez to decrypt; gaining unauthorized access to TJX's network and ultimately downloading payment card data; installing a virtual private network connection from a TJX system on to a server obtained by Gonzalez; uploading sniffer programs to a TJX payment card transaction processing server, and ultimately capturing track 2 data; and obtaining payment card transaction data from a nearby retailer's wireless access point. Scott also faces a forfeiture proceeding relating to proceeds of his misconduct, which include approximately $400,000 and myriad jewelry and computer hardware. Upon information and belief, Scott is a cooperating witness for the government.

Damon Patrick Toey pleaded guilty to a four-count Information charging Conspiracy and three underlying counts. Beyond his conduct described at length in the PSR, his overt acts in furtherance of the conspiracy include selling victims' credit and debit card information ("dumps") on Gonzalez's behalf and splitting the proceeds; collaborating with Gonzalez on Internet-based attacks, the purpose of which was to find

vulnerabilities in corporate computer networks and steal track 2 data and accounts and files; and gaining unlawful access to a Forever 21 retail server, and then providing that access to Gonzalez for the purpose of stealing customers' credit card information. Toey's concurrent forfeiture action includes approximately $9,500 and various computer and electronic hardware. He has admitted to making approximately $80,000 for his involvement in this conspiracy. Toey is a confirmed cooperating witness.

Maksym Yastremskiy and Aleksandr Suvorov are charged along with Gonzalez in the 27-count indictment in the Eastern District of New York (case no. 08-cr-00160). These defendants are alleged to have conspired to gain unauthorized access to Dave & Buster's, Inc. point-of-sale servers and ultimately acquire track 2 data, which they in turn sold or used to make fraudulent purchases. The defendants accomplished the acquisition of track 2 data by using "packet sniffers" in many different servers. As detailed by the PSR, Yastremskiy was a source for Gonzalez to sell track 2 data acquired from Scott's OfficeMax intrusions. There is no allegation against Watt in that case.

Jonathan Francis Williams pleaded guilty to an eight-count superseding indictment in the Eastern District of Pennsylvania charging him with direct counts of possession of counterfeit access devices and aggravated identity theft, as well as two firearms-related counts. Williams used fake debit/credit cards to access ATM's and withdraw or attempt to withdraw cash. As detailed in the PSR, Williams assisted Gonzalez by cashing out the debit cards obtained from the OfficeMax intrusions; he was arrested in Philadelphia with $200,000 in such "cashing out" proceeds. He received a 5-year sentence after his plea, which is the maximum sentence that Watt faces in the instant matter.

Jeremy Jethro was recently charged in a one-count misdemeanor Conspiracy Information for allegedly providing Gonzalez with a "zero day exploit" program, and receiving $60,000 from Gonzalez for doing so. The Information states the purpose of the "zero day exploit" program as follows: "to take advantage of an unknown or unpatched security vulnerability in Microsoft's Internet Explorer web browser and enable the conspirators to unlawfully gain access to, and redirect, individuals' computers." At first glance, this may seem to be analogous to Watt's case. It is not – Jethro's actions were far more dangerous and complex. The type of software supplied by Jethro takes advantage of a publicly unknown and undocumented security flaw in Microsoft's Internet Explorer, which is by far the most widely used Internet browser in the world. The term "zero day" describes the novelty of the software: it is "zero days" old, or previously undiscovered. This exploit allows a malicious party to infect a popular website with data that would assume full control over any computer that visited such website with the vulnerable Internet Explorer browser (and an unlimited number of computers, at that). As this type of software vulnerability would be extremely pervasive and easy to exploit, the program developed to do so would be highly coveted and valued (as demonstrated by the hefty price tag of $60,000). Such a vulnerability as this one would have most likely taken many weeks, or even months of painstaking auditing of the Internet Explorer application to discover. Even after the vulnerability was found, it would have most likely taken anywhere between several days to even many weeks to make a successful software

exploit for the vulnerability. Microsoft employs its own full-time staff of security experts to find these vulnerabilities in Internet Explorer, and to patch them before they are discovered by outsiders. Additionally, this class of Internet browser exploits is considered a sort of "holy grail" by security experts who are attempting to create a name for themselves through their cutting edge research. As a result, it would clearly take an expert to find a vulnerability in such a piece of code, and it would certainly be a time-consuming process. Accordingly, Jethro's actions, for which he faces a misdemeanor charge, stand in stark contrast to Watt's, which involved work on an elementary sniffer program (for no money) as detailed above.

Humza Zaman was recently charged in a one-count Conspiracy Information for allegedly repatriating to Gonzalez approximately $38,000 from Latvian bank accounts specified by Gonzalez, and keeping a 10% commission for himself; flying to California at Gonzalez's direction, picking up approximately $300,000 in repatriated proceeds, and shipping the funds to Gonzalez in Florida; and transmitting to Gonzalez ATM system logs of the bank at which Zaman was then employed for the purpose of determining whether such information would be of value to Gonzalez or his co-conspirators.

The foregoing summary of the co-conspirators in this matter, and the financial benefits they reaped from their efforts, reveals the tangential and inconsequential nature of Watt's role. The same can be said of Watt's actions standing alone, even without the benefit of the aforementioned comparisons.

III. The Defendant's Plea

Watt pleaded guilty on December 22, 2008 to the sole count of his Information, under a plea agreement dated October 7, 2008 (a copy of which has been provided to the Court as an attachment to the PSR). Under this agreement, Watt admitted only to the following limited overt acts:

> a. On diverse dates, WATT modified for Albert Gonzalez and provided to him a sniffer program used by the conspirators to monitor and capture data traveling across corporate computer networks.
>
> b. In January, 2008, Watt edited the "blabla" sniffer utilized by the conspirators, which was stored in a server assigned the ip address 195.3.144.9, located in Latvia.

The plea agreement states that the parties have no agreement with respect to the application of the U.S. Sentencing Guidelines (hereafter, the "Guidelines"), with the exception of the government's agreement to recommend that the Court reduce by three levels Watt's Adjusted Offense Level under U.S.S.G. §3E1.1.

IV. The Pre-Sentence Investigation Report and Watt's objections

In sum, the PSR concludes that Watt's proper Total Offense Level is 43 (PSR para. 55) and that no factors are known that may warrant departure (PSR para. 136).[3] These conclusions are made while at the same time recommending a reduction for Watt's minor role in the offense (PSR para. 50), and recognizing that Watt faces a maximum sentence of five years incarceration despite the life sentence normally associated with offense level 43 (PSR paras. 115, 116).

These contradictions inherent in the PSR make it objectionable on its face, and indicate that the Probation Office's and the government's calculations severely overstate Watt's degree of culpability and need for correction. Before addressing the question of departures and the appropriate analyses of the 18 U.S.C. §3553(a) factors in this case, however, it is appropriate to first detail Watt's objections to the PSR's findings as a matter of law and present the resulting Guidelines calculation that Watt proposes.

Watt's objections, documented in the PSR submitted to the Court, are further articulated as follows:

1. The PSR's loss calculation under U.S.S.G. §2B1.1(b)(1) does not reflect an extent of harm that was reasonably foreseeable to Watt: The PSR concludes that an increase of 30 levels is appropriate, based on the assumption that the full measure of losses inflicted by Watt's co-conspirators must be attributed to him (PSR para. 45). Before reaching the question of whether losses involved in this matter are reflective of Watt's blameworthiness herein (which is more appropriately discussed in the context of 18 U.S.C. §3553[a] factors and departures, below), Watt first submits that this calculation should be rejected as a matter of law.

   The proper meaning of "loss" under the Guidelines is "the greater of 'actual loss,' defined as the 'reasonably foreseeable pecuniary harm that resulted from the offense,' and 'intended loss,' defined as 'the pecuniary harm that was intended to result from the offense.'" *U.S. v. Marti-Lon*, 524 F.3d 295, 301 (1st Cir. 2008), *citing* U.S.S.G. §2B1.1(b)(1) cmt. n. 3(A)(i)-(ii) (also holding that the District Court correctly found that the harm caused by the defendant was a "direct result of the offenses for which defendant was convicted..." and that the loss was "an integral part of defendant's illegal scheme").

   Watt submits, based upon the factual arguments already presented in this memorandum, that the pecuniary harm suffered in this case was not a reasonably foreseeable result of his providing the sniffer program to Gonzalez. Just as importantly, Watt argues that the government cannot

[3] Please note that I have not seen the finalized PSR. As such, I cannot know what final recommendations the Probation Office will make, either with regard to departures or an appropriate sentence under 18 U.S.C. §3553.

establish to what extent, if any, that such losses were reasonably foreseeable to him. While it may be reasonable to speculate that *some* measure of pecuniary harm was foreseeable to Watt as to *someone* or *some* entity, such speculation cannot carry the government's burden to prove that the loss was a "direct result of the offenses for which defendant was convicted..." *U.S. v. Marti-Lon*, 524 F.3d at 302. *Cf.*, *U.S. v. Curran*, 525 F.3d 74, 81 (1st Cir. 2008) (holding that it was reasonable to conclude that payments made by victims of a phony medical doctor for fraudulent services were actual losses resulting from the offense). If the Court cannot even estimate *how much* "harm" was foreseeable to Watt, then it would be improper to arbitrarily assign such an amount for purposes of calculating his offense level.

Moreover, Watt submits that his arguments are not defeated by application note 3(F)(i) to U.S.S.G. §2B1.1. Said note determines that "loss" in cases involving unauthorized access devices "includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than $500 per access device." The government presents no evidence that any particular amount of loss resulted from unauthorized charges, or that any particular number of devices were used to make unauthorized charges. Moreover, Watt's particular conduct did not involve unauthorized access devices. For these reasons, and for the reasons articulated below with regard to 18 U.S.C. §3553(a), applying a $500 minimum loss to the millions of devices involved in this matter would be improper as well as unjust.

Accordingly, Watt requests that the Court reject the PSR's recommendation that a 30 level increase under U.S.S.G. §2B1.1(b)(1) be imposed, and he submits that no increase can be definitively assessed under this section as a matter of law.

2. Watt's objection to the PSR's loss calculation based on insufficient sources of loss information: Watt initially submitted objections to the first disclosure of the PSR, which referenced various corporate 10-K filings in 2007 and 2008 as its bases for establishing loss amounts. Watt has since been provided with TJX's 2009 10-K filing, which seems to contain more definitive information relating to that company's loss, beyond mere estimates. Therefore, Watt defers to Your Honor's discretion as to whether and to what extent such information is sufficient to allow the Court to "make a reasonable estimate of the range of loss, given the available information." *See U.S. v. Curran*, 525 F.3d at 78.

3. No increase under U.S.S.G. §2B1.1(b)(2) should be imposed: Defendant objects to the PSR's determination that "the offense involved more than 250 victims" and, therefore, that "a six-level increase is warranted" under U.S.S.G. §2B1.1(b)(2)(c) (PSR para. 46). No substantive information is

provided by the government's offense conduct statement relating to victims other than the four corporate victims, and no nexus between Watt's offense conduct to additional victims is presented. General statements relate to individual and bank victims, however nothing further is provided. The government, moreover, did not cite any victim adjustment in its Guidelines calculations submitted to the Probation Office.

Accordingly, Watt requests that the Court reject the PSR's conclusion that a 6 level increase be imposed, and instead submits that no increase be assessed under U.S.S.G. §2B1.1(b)(2).

4. No increase under U.S.S.G. §2B1.1(b)(10)(B)(i) should be imposed: Watt respectfully requests that the Court reject the PSR's conclusion that a 2-level increase be imposed, "since the offense involved the trafficking of unauthorized access devices" (PSR para. 48). Watt submits that no increase be assessed under U.S.S.G. §2B1.1(b)(10). His offense conduct did not involve production or trafficking of any unauthorized access devices.

5. Watt's role should be characterized as minimal under U.S.S.G. §3B1.2: Watt objects to the determination that he is entitled only to a 2-level minor role reduction. As argued earlier in this memorandum, Watt's role in this conspiracy was minimal. He was plainly the least culpable of all those involved, and the type of technical assistance he provided to Gonzalez was of an elementary and readily available nature.

   "Courts have identified two referents for determining role: First, one must look to other participants in the offense of conviction. *See United States v. Martinez-Vargas*, 321 F.3d 245, 250 (1st Cir. 2003). Second, one must look to whether the defendant is 'less culpable than most other persons convicted of comparable crimes.' *Id.* at 250; *see also* U.S.S.G. §3B1.2 cmt. n.3(A)." *U.S. v. Cabrera*, 567 F.Supp.2d 271, 277-278 (D.Mass. 2008). Watt's actions as compared to other participants in this conspiracy were clearly minimal. With regard to an "average participant" in a typically comparable case, the actions of someone who would provide a program such as an elementary sniffer without remuneration or desire for profit is certainly akin to someone being at the bottom of the hierarchy. *See U.S. v. Cabrera*, 567 F.Supp.2d at 278.

   Based on these analyses, therefore, Watt requests that the Court reject the PSR's conclusion that only a 2-level reduction be applied, and instead grant him a 4-level reduction under U.S.S.G. §3B1.2 (a).

6. Remaining objections or notations: Watt reserves any remaining objections until time of sentence. I have not had the opportunity to review the final version of the PSR prior to submitting this memorandum.

7. Watt's resulting proposed Guidelines calculation: As a result of the above-described objections, Watt proposes the following Guidelines calculation in this matter:

Base offense level (USSG §2B1.1[a][2])	+6
Loss calculation/relevant conduct (USSG §2B1.1[b][1])	+0
Involved sophisticated means (USSG §2B1.1[b][9][c])	+2
Trafficking unauthorized access devices (USSG §2B1.1[b][10])	+0
Use of special skill (USSG §3B1.3)	+2
Acceptance of Responsibility (USSG §3E1.1[a])	-2
Minimal Role (USSG §3B1.2[a])	-4
TOTAL:	4

Watt is mindful that the Court will, in all likelihood, wish to assess a loss enhancement despite Watt's objections. I will present further argument on this subject at the sentencing hearing.

V. Analysis of 18 U.S.C. §3553(a) factors and relevant departures

Should the Court reject Watt's proposed Guidelines calculations and underlying legal objections, Watt respectfully submits that he should be sentenced outside and below the determined Guidelines range based upon the facts of this particular case and his specific characteristics. Watt avers that a period of incarceration is not needed "to reflect the seriousness of the offense, to promote respect for the law[,]" "to afford adequate deterrence to criminal activity[,]" or "to protect the public from further crimes of the defendant." *See* 18 U.S.C. §3553(a)(2)(A)-(C).

In accordance with the Supreme Court's decision in *United States v. Booker,* 125 S.Ct. 738 (2005), and the First Circuit's decisions in *United States v. Pelletier,* 469 F.3d 194 (1st Cir. 2006) and *United States v. Vargas*, 560 F.3d 45 (1st Cir. 2009), *et. al.*, the sentence to be imposed must include consideration of all of the factors identified in 18 U.S.C. §3553(a), including the advisory Sentencing Guidelines established by the United States Sentencing Commission. In order to impose a sentence "sufficient, but not greater than necessary" the Sentencing Guidelines are merely advisory, and a sentencing court must consider the Sentencing Commission's intent as just one of several salient factors in determining whether to impose a Guideline sentence or a non-Guideline sentence and the length of such a sentence. *See* 18 U.S.C. §3553(a)(5)(A); *United States v. Booker,* supra. "In particular, section 3553(a)(1) asks that the sentence imposed consider both 'the nature and circumstances of the offense and the history and characteristics of the defendant,' while section 3553(a)(2)(A) demands that the penalty 'provide just punishment for the offense' that simultaneously 'afford[s] adequate deterrence to criminal conduct' as required by §3553(a)(2)(B)." *United States v. Serrano,* 2005 WL 1214314 at *5 (S.D.N.Y. 2005). *See also, United States v. Marsh*, 561 F.3d 81 (1st Cir. 2009).

Indeed, the Policy Statement of U.S.S.G. §5K2.0 provides a formula for considering what is relevant in constructing a reasonable sentence pursuant to 18 U.S.C. §3553, stating:

> [a]n offender characteristic or other circumstance that in the Commission's view, "not ordinarily relevant" in determining whether a sentence should be outside the applicable guideline range may be relevant to this determination if such characteristic or circumstance is present to an unusual degree and distinguishes the case from the "heartland" cases covered by the guidelines in a way that is important to statutory purposes of sentencing.

In *United States v. Broderson*, 67 F.3d 452 (2nd Cir. 1995), the Second Circuit explained that pursuant to U.S.S.G. §5K2.0, even in cases in which no single mitigating circumstance is, itself, sufficient to warrant an adjustment, the district court has the authority to construct a sentence based on a combination of such circumstances. *See also, United States v. Bradstreet*, 207 F.3d 76, 82 (1st Cir. 2000) (noting that the Sentencing Commission does not intend to limit the kinds of factors that could constitute grounds for departure in an unusual case); *United States v. Rioux*, 97 F.3d 648, 663 (2d Cir. 1996) (upholding district court's conclusion that, in combination, defendant's medical condition and charitable and civic good deeds warranted downward departure); *United States v. Lombard*, 72 F.3d 170 (3rd Cir. 1995) (particular combination of circumstances culminated in "unusual" Guidelines calculation mandating an otherwise unreasonable life sentence); *United States v. Sclamo*, 997 F.2d 970 (1st Cir. 1993) (extraordinary family circumstances warranted departure), citing *United States v. Rivera,* 994 F.2d 942 (1st Cir. 1993); *United States v. McGee*, 802 F. Supp. 843 (E.D.N.Y. 1992) (substantial downward departure to avoid imprisonment was justified for a defendant who pleaded guilty to importing 244.1 grams of heroin, where the defendant was a productive member of work force, continued to educate herself, incarceration would damage defendant's nephew, and defendant's contrition was exceptional).

Watt's grounds for departures and consideration under 18 U.S.C. §3553 include: 1) the great disparity between the overall losses suffered in this matter and his measure of culpability herein; 2) the minimal nature of his participation in this offense, including his lack of profit from the object of the conspiracy; 3) the irreparable harm and, therefore, the severe punishment that has already resulted from his felony conviction; 4) his young age during the period relevant to this conspiracy; 5) the extreme likelihood that he will not recidivate; and 6) the disparity of punishment that a lengthy sentence of incarceration would represent as compared to other similarly situated defendants.

1. <u>The PSR's loss amount grossly overstates Watt's culpability and need to be corrected</u>

Your Honor has vast experience with reviewing questions of loss as they relate to defendants' culpability, need for deterrence, incapacitation, just punishment and rehabilitation. *See, e.g., United States v. Mueffelman*, 400 F.Supp.2d 368, 378 (D.Mass.

2005). Indeed, Your Honor noted the following with regard to the general principles relating to loss and a defendant's culpability:

> The amount of loss that a given crime has engendered is surely one measure of the seriousness of the offense. Sometimes loss is an entirely appropriate proxy for culpability. At other times, it is not. All other things being equal, one who causes a greater loss as a result of his or her illegal acts is more culpable than one who causes a lesser loss. But, as Judge Lynch noted in *United States v. Emmenegger*, 329 F.Supp.2d 416, 427 (S.D.N.Y. 2004), 'in many cases...the amount stolen is a relatively weak indicator of the moral seriousness of the offense or the need for deterrence.'
>
> *United States v. Mueffelman*, 400 F.Supp.2d at 373.

Moreover, in the context of applying a 18 U.S.C. §3553(a) analysis with regard to loss, Your Honor has noted the following:

> Nonetheless, as Judge Lynch's decision in *United States v. Emmenegger* suggests, issues concerning the blameworthiness of a defendant found guilty of fraud are more complex than simply measuring the amount of the loss. Indeed, even pre-*Booker,* loss was not an automatic measurement of culpability. For example, Guideline law permitted a judge to consider whether the amount of loss overstated defendant's culpability. *See* U.S.S.G. § 2B1.1, Appl. Note 19(C). *See, e.g., United States v. McBride,* 362 F.3d 360 (6th Cir.2004) (explaining that although intended loss drives offense level even where scheme to defraud could not have succeeded, impossibility of scheme can be a basis for departure); *United States v. Lauersen,* 348 F.3d 329 (2d Cir.2003) (holding that where multiple adjustments result in very high offense level that substantially overstates seriousness of offense, district court may depart downward); *United States v. Gregorio,* 956 F.2d 341 (1st Cir.1992) (holding that downward departure is appropriate where degree of loss was caused by downturn in economy); *United States v. Graham,* 146 F.3d 6 (1st Cir.1998) (holding that loss overstates culpability where lower loss attributed to similarly situated defendants); *United States v. Monaco,* 23 F.3d 793 (3d Cir.1994) (explaining that loss overstates seriousness where defendant had no intent to steal); *United States v. Stuart,* 22 F.3d 76 (3d Cir.1994) (affirming loss calculation based on face value of stolen

> bonds, but suggesting appropriateness of departure on remand where defendant received little money for participation in offense, causing loss to overstate seriousness of offense).
>
> This approach – treating loss as a contingent factor, whose significance depends on the circumstances – is especially salient post-*Booker*. With advisory Guidelines, the amount of loss should be understood in the context of the purposes of sentencing enumerated in 18 U.S.C. § 3553(a), including deterrence, incapacitation, just punishment and rehabilitation, as well as the need to provide restitution to any victims of the offense.
>
> *United States v. Mueffelman*, 400 F.Supp.2d at 377-378.

Your Honor's decision in the *Mueffelman* case was only one such analysis you have conducted with regard to the principles relating to loss and defendants' culpability and need for correction. For example, in the pre-*Booker* case of *United States v. Costello, III, et. al.,* 16 F.Supp.2d 36 (D.Mass. 1998), Your Honor noted that "the 'heartland,' in effect, resides in a case where loss and gain are roughly coincident...In contrast, where the defendant is not the principal, where he or she is a functionary, loss to the victim and gain to the defendant are not comparable....Other courts have described this in terms of the extent to which the harm, defined by the loss, overstates the culpability of the defendant." *See United States v. Costello, III, et. al.,* 16 F.Supp.2d at 39. Your Honor further cited in that decision to the case of *United States v. Stuart,* 22 F.3d 76, 83 (3rd Cir. 1994), for the following premise: "where application of the Guidelines' monetary table bears little or no relationship to the defendant's role in the offense and greatly magnifies the sentence, the district court should have the discretion to depart downward.'" *United States v. Costello, III, et. al.,* 16 F.Supp.2d at 39, citing *United States v. Stuart*, ibid.

Turning to Watt's role in the instant offense and the disparity represented by the PSR's loss calculation under U.S.S.G. §2B1.1, it is clear that a substantial prison sentence as suggested by such loss calculation (even with the maximum term "capped" at 5 years under 18 U.S.C. §371) would be inappropriate based on Watt's culpability and need for correction in this case. Without seeking to rehash the detailed factual arguments already presented earlier in this memorandum, the elementary assistance Watt provided to Gonzalez, together with the entire immature and youthful context within which he provided such assistance, does not merit incarceration. This is especially so in light of the remaining factors to be considered under 18 U.S.C. §3553(a), including the severe punishment that Watt has already received for his actions.

2. Watt's minimal role in this conspiracy, his youth, the punishment that his conviction represents, and his unlikelihood of recidivism

In addition to the Guidelines implications of recognizing Watt's minimal role herein, such role merits substantial consideration when applying the factors within 18 U.S.C. §3553(a) to this case (e.g. "the nature and circumstances of the offense" and "the need for the sentence imposed to reflect the seriousness of the offense"). The same applies to Watt's youth and the extreme unlikelihood that he will recidivate.

Your Honor has certainly undergone similar analyses in the past. For example, in *Costello, III*, Your Honor noted that co-defendants Downing and Dooley did not "come up with the scheme at the outset"; their "profit, at least with in the first transaction, was miniscule compared to the value of the materials stolen"; and that they were "little more than laborers in the first transaction." *See United States v. Costello, III, et. al.,* 16 F.Supp.2d at 38-39 and 41. For those reasons, Your Honor concluded, "I have no doubt that the Government's enforcement's efforts have nipped their computer theft career in the bud." *Costello, III,* ibid at 41. Watt's situation is very similar, in that he by no means conceived or even participated in Gonzalez's conspiracy. He also did not profit from it, aside from being able to "party" with his friend. Indeed, there is no better indication of how Watt's youthfulness and mischievous immaturity led to his actions in this case than this. Watt perhaps cannot even be compared as "little more than [a] laborer," as the sum total of his actions include working on a simple software program that could have been obtained through easily accessible open source media.

These facts, together with the significant punishment he has and will continue to receive as a result of his conviction in this matter, demonstrate that Watt is entirely unlikely to recidivate. Watt spent years, academically and then in the workforce, cultivating his reputation and establishing himself within the securities industry as a software engineer with unique skills critical to the development of financial systems. He was summarily fired on the day that a search warrant was executed at his office – his employer did not even wait to determine whether Watt would be charged with any offense, much less convicted. Now, with a federal felony criminal record, Watt cannot be employed within the securities industry again, nor will any company or contractor working with or for the securities industry employ him. That particular career path has, in effect, been destroyed. The long-term damage to other paths remains to be seen, but the probabilities are quite ominous.

The consequences of Watt's actions and, subsequently, this conviction, cannot be overstated. Not only has his chosen line of work now been permanently foreclosed, Watt's prohibition against any computer use has rendered him completely unable to even attempt to find future employment. It stands to reason that a marketable computer programmer would need to use a computer to make a living – beyond that obvious point, however, Watt cannot even stay current on the latest, and legitimate, cutting-edge issues in computer engineering, which would help him remain competitive as a prospective hire. In any event, the ease with which his felony conviction will be available for any potential employer in a computer-related field to review will certainly pose a challenge to his

future success. Watt will have to start over, and hope that his skills not only will land him on his feet, but that they will do so in a field that is at least somewhat as financially promising as the career that he has lost. It is worthwhile to note that Watt should not be compared to an "IT" manager or technician – while he may be able to find such work in the "field" of "computers," it will perhaps never offer Watt the type of career that he had been building until his prosecution.

Beyond employment concerns, Watt's computer abstention has also curtailed his ability to communicate with his family, who live either out of State or out of the country. Large telephone bills are beyond Watt's ability to afford. Internet calling previously made his communication with his family easy. Watt has become withdrawn and depressed. He has also been forced to borrow huge amounts of money from his mother as a result of this prosecution. He could no longer make his mortgage payments on his residence, so his mother agreed to pay his mortgage off (at considerable expense to her, depleting her own cash reserves). Watt's mother has also paid his legal fees and contributed to his living expenses, to make up for whatever Watt's unemployment insurance cannot. Again, Watt has been unemployed since the inception of this case (August of 2008, almost 10 months now). His health has also suffered from his ordeal. He has curtailed medical care due a lack of medical insurance, despite a recurring lower back condition and a more recent wrist injury.

The foregoing information is not provided to conjure sympathy, but to demonstrate the extraordinary impetus Watt has to avoid recidivating. Even if it were possible to ignore the personal affects that this ordeal has had upon him, the objective truth is that at best, his future career prospects will face severe adversity. At worst, if he cannot use computers for the foreseeable future, any prospects he might have had, even limited ones, will be completely gone. If that were to happen he would have no idea what to do for a decent living. One would be hard pressed to devise a more frightening scenario for a young man with a once-promising future.

It is also noteworthy that Watt has no criminal record. This, and the other facts articulated above and throughout this memorandum, indicate that any concerns about recidivism do not compel a sentence of incarceration. Your Honor noted as much in *United States v. Cabrera*, 567 F.Supp.2d at 279, as follows: "The Sentencing Commission's report, *Recidivism and the 'First Offender'* (May 2004), *available at* http://www.ussc.gov/publicat/Recidivism_FirstOffender.pdf, suggests that individuals – like Cabrera – with zero criminal history points are less likely to recidivate than all other offenders. Commission studies show that the recidivism rather for such individuals is substantially lower than recidivism rates for other offenders, and even for offenders with only one criminal history point."

Watt has not touched a computer since his arraignment and plea in December of 2008, just as he has not used any controlled substance since that date. His maturation process advanced before being prosecuted in this case, with his marriage to Tena Bugarin in August of 2008 and the increased mental and emotional stability that resulted in Watt's life. He has lost his chosen career, and subsequent to this sentence he may very well lose

his liberty. Even if he is not incarcerated, he will be closely supervised by the U.S. Probation Office, not to mention his wife and his mother, who are very involved in his life. For these reasons, Watt submits that a probationary sentence affords adequate deterrence to criminal conduct and protection to the public from further crimes of the defendant. *See* 18 U.S.C. §3553(a)(2)(B) and (C).

3. Watt's sentence should be commensurate with other similar situated defendants

Watt is not privy to Your Honor's experiences with other defendants or cases involving conduct similar to that of the conspirators in this matter. As a result, Watt defers to Your Honor's determination as to whether his conduct is more or less culpable than other minimal participants, in a similar hierarchy, as compared to Watt in this conspiracy. *See, e.g., United States v. Cabrera*, 567 F.Supp.2d at 279. *See also, United States v. Garrison*, 560 F.Supp.2d 83, 84-85 (D.Mass. 2008) ("The numbers – the Guideline computation – could mask real differences between offenders, in effect, a 'false uniformity.' [citation omitted]. It is especially important, now that the Guidelines are advisory, that judges are charged with looking beyond the Guidelines categories and that they know what their colleagues have done in comparable cases. The new discretion will be influenced, as it should be, by the precedents of the court: a true common law of sentencing" [footnote omitted]).

Watt can compare his conduct, however, to that of his co-conspirators as well as against some other arguably similar cases. In this matter, for the reasons already articulated in this memorandum, it is unquestioned that Watt is the least culpable actor and, indeed, the one with the most limited participation in this conspiracy. As previously argued, the government's assertion that Watt's elementary "sniffer" program was "critical to the success of the massive identity theft which followed," seeks to inappropriately confer an enormous measure of culpability on Watt. Although none of his co-conspirators have been sentenced as of yet, the key defendants in this matter (other than Gonzalez) are cooperating and will undoubtedly receive significantly more lenient sentences by comparison to what they were facing. The remaining defendants were lesser participants, but they too were far more affirmatively involved in this scheme than Watt. In the end, each co-conspirator demonstrated an enthusiasm to further this specific conspiracy that Watt pointedly lacked.

Regarding other similar cases, there exist examples nationwide that involve "hackers" and identity thieves of varying sophistication. More difficult to find, however, are cases involving collateral actors such as Watt. For instance, in the broad investigation and prosecution of the "Shadow Crew" conspirators by the District of New Jersey from 2003 to 2006, over two dozen individuals were charged and convicted in the aftermath of the government's investigation (dubbed "Operation Firewall"), which Gonzalez assisted. The lead defendant in these cases, Andrew Mantovani, was the administrator and co-founder of the shadowcrew.com website, described as "one of the largest online centers for trafficking in stolen credit and bank card numbers and identity information" that "trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in estimated losses in excess of $4 million to victims, who ultimately were the issuing

institutions for the credit and bank cards." *See* 6-29-06 Press Release, U.S. Attorney's Office for the District of New Jersey. Mantovani received a sentence including 32 months imprisonment and a $5,000 fine (case no. 04-cr-00786). A review of the next nine conspirators named in Mantovani's indictment reveals that most of them pleaded guilty to being either a "moderator," "administrator," or "vendor" on the shadowcrew.com website, and that they trafficked in stolen credit card numbers in some manner. Of those nine, seven received jail sentences ranging from 16 months to 25 months and fines ranging from $1,000 to $2,000.

Two of those ten defendants, however, received probationary sentences. The first, David Appleyard, was also charged by the Western District of New York for similar offenses (case no. 05-cr-134). Appleyard pleaded guilty in both jurisdictions and was sentenced to concurrent terms of probation. He did not "traffic in counterfeit access devices" nor did he "financially gain" from his conduct. *See* Schedule A to Appleyard's Plea Agreement, District of New Jersey. Appleyard apparently cooperated in some manner, as an agreement to cooperate is written in to his plea agreement. He also received a $2,000 fine and 12 months of electronic monitoring.

The second defendant to receive a probationary sentence was Matthew Johnson, age 23, who "admitted to creating over 1000 false identification documents" and selling them to other shadowcrew.com members. *See* 6-29-06 Press Release, U.S. Attorney's Office for the District of New Jersey. Johnson also received a $2,500 fine.

Another recent case involved Jason Michael Milmont, age 20, who was convicted in the District of Wyoming (case no. 08-cr-00146) for creating one of the world's first "botnets" to use "peer-to-peer technology." A "botnet" is typically a network of infected computers that are used to control or attack computer systems. "Peer to peer" technology creates a computer network distributed over individual computers, as opposed to a central server. This essentially made it much more difficult for the botnet to be shut down. Milmont created malware called the "Nugache Worm," which, when spread to unsuspecting computers through a website that Milmont also created, allowed Milmont to gain control of those now-infected computers. Milmont used this access to steal access device information such as user names, passwords, and account numbers for use in committing access device fraud, such as purchasing merchandise with his stolen credit card information. Milmont offered cooperation as part of his plea agreement, and ultimately received a probationary sentence with 12 months of home confinement and $36,859.06 in restitution.

The U.S. Sentencing Commission does not delineate computer-related crimes as a "primary offense category" in its annual Statistical Information Packet. The arguably comparable offense categories to the instant matter include fraud and larceny. A review of the mean prison terms for such offenses reveals a nationwide mean of 28.6 months for Fraud offenses (28.9 months in the First Circuit), and 18.8 months for Larceny (13.5 months in the First Circuit, albeit on only 9 cases). *See* U.S. Sentencing Commission Statistical Information Packet, Fiscal Year 2008, First Circuit, Table 7, p.10, *available at* http://www.ussc.gov/JUDPACK/2008/1c08.pdf.

Watt respectfully submits that his conduct in this matter is distinct from the actions of the "hackers" involved in the aforementioned crimes, with the possible exception of David Appleyard, who did not "traffic in counterfeit access devices" or "financially gain" from his conduct. Even in the cases of defendants who have taken affirmative steps to directly perpetrate computer-related intrusions and thefts (as well as other, generic classes of frauds and larcenies), the prison sentences imposed seem to be far less than even the five-year statutory maximum facing Watt in this matter. Accordingly, Watt reiterates his prayer for a probationary sentence or, in the alternative, a minimal sentence of incarceration.

VI. Remaining Sentencing Issues

Before concluding, I wish to briefly address remaining issues such as a possible fine, restitution amount, and Watt's ability to utilize computers in the near future.

I have not had the opportunity to review the final PSR prior to submitting this memorandum. However, based on my knowledge of my client's finances, I believe it accurate to state that Watt has few assets beyond his residential apartment, which he owns outright thanks to his mother's assistance.[4] This asset is, obviously, illiquid, and would not have materialized but for Watt's mother's generosity. Watt's lack of liquid assets, his minimal role in this conspiracy, and the aforementioned lack of profit that he gleaned from his acts in furtherance of this enterprise, mitigate against the imposition of a substantial fine or restitution.

Further, regarding Watt's future computer use, argument has been submitted above that illustrates Watt's inability to earn a living or remain competitive for any job placement without being permitted to use a computer in a legitimate, law-abiding fashion. Watt's vocational expertise is in computer software engineering and development. He has already lost all opportunity for employment within the securities or financial services industries, where he was building a niche practice for the long term. He now has to "start over" in very real sense. Without access to a computer, this "starting over" will take on an entirely new and devastating meaning: he will have no choice but to re-enter the workforce without any skills to offer. Without doubt, permitting Watt to use computers in a legitimate fashion as a condition of his probationary sentence or supervised release is reasonable to ensure that he becomes a positive and productive member of society. There is equally little doubt that Watt is motivated to protect his most valuable asset – his ability to use computers – by avoiding illegal activity for the rest of his life.

---

[4] Watt has recently executed a promissory note for his mother's benefit and at his mother's request, memorializing Watt's pre-existing verbal agreement to ultimately pay his mother back for the funds she advanced to purchase his apartment, pay his legal fees, and provide other financial support to him. Watt does not expect the Court to consider this note, however, as a "liability" that would prevent him from paying a fine. The note simply illustrates that Watt lacked any wherewithal to purchase an asset such as his residence without assistance from his mother.

VII. Conclusion

For the foregoing reasons, Watt respectfully requests that the Court impose a probationary sentence in this matter or, in the alternative, a minimal sentence of incarceration. Further, Watt requests that the Court consider all arguments herein with regard to the imposition of any fine or restitution, as well as his permissible computer use in the immediate future.

Respectfully submitted,
The Defendant,
Stephen Watt,
By His Counsel:

/s/ Michael C. Farkas
Michael C. Farkas, Esq.
381 Park Avenue South, 16th Floor
New York, NY 10016
(212) 760-8400
mfarkas@farkaslawfirm.com
Lead Counsel, pro hac vice

Certificate of Service

I, Michael C. Farkas, hereby certify that on this date, June 1, 2009, a copy of the foregoing document has been served via the Electronic Court Filing system on all registered participants.

/s/ Michael C. Farkas
Michael C. Farkas